GX_____

Ollscoil na hÉireann, Gaillimh
National University of Ireland, Galway

Autumn Examinations, 2010

Exam Code(s)	4IF1
	Bachelor of Science in Information Technology
Module Code(s)	CT437
Module(s)	Computer security and forensic computing
Paper No.	1
External Examiner(s)	Prof. M. O'Boyle
Internal Examiner(s)	Prof. G. Lyons
	Dr. J. Duggan
	*Dr. C. Mulvihill

Instructions: Answer any four questions.

All questions carry equal marks.

Duration	3 hrs
No. of Answer Books	1
No. of Pages	1
Department(s)	Information Technology

Question 1
(a) Briefly explain the term 'public key cryptography' (8 marks)
(b) Explain what is meant by the term 'digital signature' (8 marks)
(c) Explain the operation of a certificate revocation list (9 marks)

Question 2
(a) What is meant by the terms 'hot site' and 'cold site'? (8 marks)
(b) Briefly explain what is meant by RAID 0 and RAID 1 (8 marks)
(c) You are tasked with providing 1000GB of storage via a RAID 1 mirroring scheme. If the disks are standardised at 500MB, explain how many will be needed (9 marks)

Question 3
(a) Explain what is meant by the term 'dictionary attack' (7 marks)
(b) Explain why logs are useful in security work? (7 marks)
(c) Work files are typically deleted once a week by your users. However only 40% of the time does this prove to be a problem; in the remaining 60% of cases there is no cost. In the 40% of cases, it takes the user on average three hours work to restore the file's contents, at a cost of 100 euro per hour. Determine the Single Loss Expectancy, the Annualised Rate of Occurrence, and hence calculate the Annual Loss Expectancy. (11 marks)

Question 4
(a) Explain what is meant by the term 'Mandatory Access Control'? (7 marks)
(b) Explain what is meant by a 'Chinese wall' (8 marks)
(c) You are developing a physical access control policy for your organisation. Discuss any three elements that might apply. (10 marks)

Question 5
(a) Explain the following terms: 'Trojan Horse', 'Worm' (9 marks),
(b) Explain what is meant by a 'keystroke logger' (7 marks),
(c) You have been tasked with developing a honeynet for your organisation. Explain what this means and how it would be used. (9 marks),

Question 6
(a) Explain what is meant by the 'chain of custody' (7 marks),
(b) Explain what is meant by 'jailbreaking' (7 marks),
(c) It appears that someone in the organisation has been using USB sticks to make unauthorised copies of information. Is there anything you can advise in connection? (11 marks)

Question 7
An entrepreneur developing software for the biomedical engineering sector has secured funding and is setting up in the west of Ireland. You have been retained to provide initial advice on a security profile. Discuss a report you might draft, making use of the following three headings: general IP protection (8 marks), laptop policy (8 marks), password policy (9 marks).